Configuration and Data Management Process and the System Safety Professional

C. Herbert Shivers, Engineering Directorate, Engineering Systems Department, Configuration and Data Management Group, Marshall Space Flight Center, Alabama

Keywords: risk management, configuration management, data management, verification, validation

Abstract

This article presents a discussion of the configuration management (CM) and the Data Management (DM) functions and provides a perspective of the importance of configuration and data management processes to the success of system safety activities. The article addresses the basic requirements of configuration and data management generally based on NASA configuration (1) and data management (2) policies and practices, although the concepts are likely to represent processes of any public or private organization's well-designed configuration and data management program.

Introduction

System Safety analyses are inherently dependent on data received from the various project support disciplines. Project data must be timely and accurate and must reflect the reality of the status of hardware, software, and data. Baseline designs and the following changes must be carefully managed and controlled in a disciplined process involving input from all associated with the successful completion of a project. System Safety professionals must be intimately involved in the process.

Configuration and Data Management Concepts

Configuration management has its roots in the early days of mass production with the advent of interchangeable parts. CM processes are built around four elements - identifying, controlling, accounting, and verifying program/project requirement baselines throughout the item's life cycle. A disciplined approach for identifying, controlling, accounting, and verifying the design, build, change, and operations processes is necessary for satisfactory results.

Data management was born of necessity to provide a means for making sure all information is accurate, current , and available to project team members. DM also functions in a contractual scenario to provide enforceable leverage for a contracting organization to get the products for which they are paying. As the world becomes inundated with more and more information, the DM function is even more important to allow accurate decisions to be made about what information is useful and what information should be set aside or discarded.

Configuration and Data Management programs provide a formal and disciplined approach to achieve these objectives. Through the CM and DM processes, management has visibility into the true status of the project throughout its life cycle.

Configuration Management: Configuration management must be a rigidly sustained discipline throughout the life cycle of a program/project. The program or project must accurately define and document the approved technical documentation of items.

The four configuration elements or processes for identifying, controlling, accounting, and verifying are instituted in a disciplined manner to ensure that the project hardware and software design and build are accurately documented and accurately reflect the product that has been delivered. The processes also provide historical records of the design baseline, changes made thereto and waivers or deviations approved as the product life cycle continues. CM is one of the most critical processes supporting a project. Analyses performed on the wrong hardware or hardware that no longer is represented by the design drawings being used are, obviously, worthless, and perhaps, even harmful.

NASA defines CM as, " the management discipline intended to define and document requirements, control changes thereto, and provide systematic accounting and verification to assure that final product (as-designed, as-delivered, as-built, etc.) satisfies established requirements (3)."

CM is the systematic process that identifies, controls, accounts for, and verifies the project or product design. CM activities begin in the project conceptual and definition phases and continue throughout the life cycle, including operations and disposal. In the initial phases of the life cycle, configuration items are identified. As the project progresses, changes to these items, and additionally identified items are controlled and tracked.

Similarly, System Safety is a systematic process that identifies, controls, tracks and verifies the control of hazards associated with the project or product. System Safety processes and CM processes are similar in their systematic implementation and a good CM program is essential to successful System Safety Program implementation.

Data Management: Data Management is simply the management of data (2). Data consists of deliverable data, in the case of a contracted effort, and data associated with project management itself in the case of both in-house and contracted efforts. Deliverable data is information and documentation required to be from a contractor in accordance with a contract. Project data is the information produced and stored by the project activities that reflects design and production status, test results, etc., that take place in the project life cycle. From either the data producer's point of view or the data receiver's point of view, a disciplined process for identifying, collecting, validating, and producing correct data is essential to project success.

Systems Safety analyses are dependent on the data accurately representing the state of the design and product configuration as well as test data, etc., that might impact previously identified hazard controls and verification activities. In addition, the data provides an historical record of changes to design features that must be considered for impact to hazard analyses. Data and information are frequently used interchangeably and include administrative, management, financial, scientific, engineering, operational, and logistical information and documentation.

System Safety Professionals and the CM and DM Processes

A project requires a clear objective for existence. That objective is further delineated in a series of requirements that, when implemented, produce the end product desired. Data management processes are employed to make sure the required information is known, planned for, and provisions are made for receipt and review of that data. The data provide the basis for which the project baselines are developed and controlled through the configuration control processes. The CM processes also create data as the project matures and that data is managed with the DM processes.

The CM and DM processes provide that all project team members know what is being produced, know the current design baseline, know the planned tests and test configurations, and know the product actually delivered. The status of all the facets of the product are also known through the CM and DM processes as changes occur.

The System Safety Professional (SSP) plays an important role in all facets of CM and DM. Requirements flow from top objectives and policies into contractual terms and provisions or in-house project requirements. The contractor or project manager must implement systems and operating processes that ensure the requirements are met. In the early stages, in both in-house and contracted efforts, the SSP must participate in the identification of data requirements and baseline design requirements to be incorporated into the product.

Configuration and Data Management Plans: Some tools created early in the life cycle for the implementation of CM and DM processes include the CM Plan and the DM Plan. Approaches and concepts are clearly defined and communicated between the procuring organization and the contractor or among team members for in-house efforts in the CM and DM Plans. The purpose of the Configuration and Data Management Plans is to define the concepts, requirements, processes and data needed for implementing and maintaining configuration on the respective program/project. The scope of the plan is the complete life cycle for the program or project. The SSP should review those plans to make sure the processes are sound and will support the SSP in activities associated with systems analyses.

Identification: Configuration identification is the definition and establishment of the baseline plans, requirements, and configuration items that will be controlled. During the configuration identification process, the SSP evaluates the proposed design and submits inputs in forms such as Preliminary Hazard Analyses to make sure a safe product is being conceived and to effect early changes to the design baseline. The SSP evaluates the intended function of the product and also the interfaces of the various planned subsystems to ensure that hazards are identified and eliminated, or controlled. The SSP also provides input into identifying data required and reviewing design and other project documents for impacts. Normally, this function can take place in conjunction with requirements reviews and preliminary design reviews handled as a program process.

Configuration identification is established by all the baseline documents necessary to provide a full technical description of the characteristics of the item that requires control at the time the baseline is established, plus all changes. Documentation necessary for defining the technical design requirements may include:

Specifications

Engineering drawings

Process specifications and processes

Contract requirements

Interface control drawings and specifications

The System Safety Professional has a vital and mandatory role in providing input to establishing these baselines and assessing the safety impact of changes.

Data requirements also are a prime area for input from the SSP in the configuration identification of a program/project. Data requirements are defined whether the project is in-house or contracted, with the specific SSP involvement defined based on the type of project and type of data involved. Some of the types of data required may involve SSP development or review and comment while others that are retained by the contractor may involve some level of SSP insight. Data requirements may include:

Documents submitted for approval to the appropriate office or activity having final approval authority over concepts, techniques, and requirements. Written approval is the norm for this type of document.

Documents allowing the contracting organization a specified time limit to disapprove the contents or issues. Typically, this type of document is distributed to provide management visibility and control as well as to permit needed coordination, integration, and review.

Documents providing information or data that the contracting organization has identified for delivery or availability on an as-needed basis.

Contractor data produced and used in the performance of the contract and normally retained by the contractor per the contract.

Documents providing data that are incidental to the performance of the contract and normally retained by the contractor as specified in the contract.

Change control: As the project progresses and as the product design matures, the inevitable changes will occur. Change processing is usually handled through a systematic effort that ensures that proposed changes can be identified, distributed to the appropriate disciplines for impact review, evaluated from a systems perspective based on inputs and interface impacts, and a disposition agreed to by project management. Implementation of the change disposition is documented and verified.

The SSP is a vital part of the change review process for accommodating engineering changes. The role of the SSP is to initiate changes, review proposed changes for impacts to the safety of the system, or impacts to the hazard analyses or other related analyses, etc.

Configuration control is the second configuration management process and involves control of the baseline established during identification. The baseline (plus approved changes) is the point or state from which all future evaluations are made. NASA defines configuration control as, "The formal process used to assure discipline in making changes to the baseline. This control is effected through formal configuration control boards (1)."

Changes to the baseline must be accomplished in an established and disciplined manner and are made to:

Correct deficiencies discovered during production

Improve materials or processes

Ensure requirements are being met

Revise hazard analysis information

All baseline changes must be carefully defined and thoroughly evaluated to determine if ripple effects that affect system elements throughout all stages of production from design to final packaging, delivery, and operations exist. The SSP must be vigilant to assess impacts to system safety.

Changes must be implemented in a controlled manner, must be effectively coordinated with related components to assure that the system remains compatible, and must be documented. Configuration control assures that these events happen. Configuration control also provides the control necessary to prevent the implementation of unauthorized changes.

Configuration control is a disciplined process used to change established baseline requirements through established procedures. The procedure may include control boards made up of member representatives of all disciplines including System Safety. A senior program or project management official usually acts as the chair and approves and directs change implementation. A hierarchy of boards may be necessary to fully affect all configuration control throughout the program. For contracted efforts, the contractor and the contracting organization will likely have their own control boards with insight and participation defined in the contract. The SSP must be involved in all levels of the change control process.

Configuration management documentation is critical to provide for the disciplined control process to succeed. Typically forms are developed and used to standardize the steps of the process. Some forms might include change request forms, change proposal forms, field change forms, deviation or waiver forms, change evaluation forms, document change forms, specification change forms, interface revision forms, and directive forms for change implementation. All these forms have different functions, but may not exist separately but rather as combination forms that might be developed. The SSP must be aware of and know how to use each form in the process.

Configuration Status Accounting: Configuration accounting or configuration status accounting is the third configuration management process and functions throughout all phases of configuration management to integrate and correlate identification, change, and verification data. Configuration accounting is necessary to effectively manage configuration items in a clear, concise, and timely manner. Configuration accounting reports are used in reviews to assure that the product meets all specified requirements. Configuration accounting systems process information at the conclusion of an audit or review that identifies the audit or review, the current status, and disposition of action items.

NASA defines configuration accounting as, "Definition and reporting of the exact baseline on a continuing basis and provision of a clear audit trail from the authorization of changes to the affected documentation and products. Accounting provides the single authoritative source for definition of the configuration baseline (1)." The SSP must make sure that the agreed to information relating to the safety analyses has been properly documented in the baselines and implemented changes.

Configuration accounting processes are established to receive, maintain, sort, correlate, and disseminate configuration documentation. The closed-loop accounting system must provide an accurate, complete, and up-to-the-minute "snapshot" of any configuration item as it progresses and matures. Included is certain mandatory information such as system safety analysis data and plans.

Usually the configuration accounting data includes both the as-designed and the as-built data. Both of these sets of data are useful and necessary to the SSP in preparing the complete and accurate System Safety Analysis. The accurate listing of baseline documentation is usually maintained through an engineering release system that includes both the as-designed and the as-built. The as-built provides the actual physical and functional status of the hardware and software, including modifications.

Comparisons between the two sets of information are input to the SSP in developing the hazard analysis. Other types of data may include as-delivered, as-tested or as-launched depending on the systems adopted. Audit trails are produced by project records that maintain the status of changes being managed by the project. These records track changes from acceptance through verification of change implementation.

Obviously, the data management systems associated with the configuration accounting process are important. Some of the data managed includes document master lists, engineering release listings, as-designed requirements, as-built documentation, current listings of actual as-built configuration item requirements (As-Modified, As-Tested, As-Qualified, As-Delivered), approved configuration baseline documentation and approved changes, an audit trail that clearly explains and authenticates any difference between as-designed requirements and as-built requirements, and the status of all proposed changes, deviations, and waivers to the approved baseline. The managed data is essential for the accuracy of the System Safety Analyses. Much as the SSP's work spans the life cycle of the program or project, so do the configuration management and the data management processes.

Configuration Verification: The actual status of the design and build must be validated to confirm the configuration. An audit or review can be used to ensure the product's compliance with requirements, both physical and functional characteristics, including those imposed through the SSP products such as the Hazard Analysis.

Confirmation is needed to ensure that the developed product does match the desired baseline and its documentation. A rigid process of verification audits and reviews provides assurance that the baseline requirements have been satisfactorily implemented for the product and that the product has been designed, developed, built, and tested properly.

NASA defines configuration verification, "A process using test, analysis, and/or inspection to confirm that a system and its hardware and software components satisfy all specified performance and operational requirements(1)." The objectives of configuration verification are to verify that baseline requirements are properly implemented, that the baseline requirements are accurate and current, and that the configuration item product is certified as having been designed, developed, built, and tested to the baseline configuration.

Configuration verification is accomplished through a series of technical reviews and audits. The processes followed will be determined by the program or project and usually are well-established processes adopted by the parent organization. Technical reviews and audits are generally employed to accomplish the task. The SSP is involved in the auditing or review process, both from the standpoint of making sure the configuration and data management processes have worked relative to accurately documenting the results of the hazard analysis, control and verification processes, and that the product is as documented. That is, the actual product is the configuration analyzed and documented.

Technical verification reviews are usually formal and specified in project plans or in contracts for out of house projects. The technical reviews usually take place at project milestones and involve in depth review, or at least an accepted level of insight, by all disciplines, including System Safety. Some typical types of review include System Requirements Review, Preliminary Design Review, Critical Design Review, Design Certification Review, Configuration Inspection, Acceptance Review, Test Readiness Review, etc.

Audits are also used to ensure accurate implementation of design requirements and changes. Some frequently used audits are the Functional Configuration Audit (FCA) and the Physical Configuration Audit (PCA). The FCA is used to verify that the item has achieved the requirements specified in its functional and allocated configuration documentation. The PCA is the formal examination of the "as built" configuration of a configuration item to determine if it conforms to the technical documentation defining the configuration item ("as-designed").

The technical reviews and audits provide the SSP a timely opportunity to make needed inputs so that the other disciplines can incorporate needed changes and to ensure, at the later stages, that the hazard analysis is accurate and that the system hazards are controlled. The SSP typically will assess the design review process, judge the maturity of the design to proceed to subsequent project milestones, identify design interfaces and controls established, review discrepant conditions and planned corrective actions. The SSP accomplish this task in part by reviewing and approving drawings, specifications, and appropriate program/project-related documentation to ensure compliance with organizational or contractual requirements. The SSP requires insight into the contractor processes for out of house projects and must make inputs to project management relative to concerns in the contractor's system safety activities as well. The contractor normally schedules and conducts management reviews/audits in which the SSP should participate or into which the SSP has insight.

The reviews require formal documentation which will be managed as a part of the Data Management process. The documentation becomes a part of the historical record and also is available for review by any project team member needing such information to incorporate changes or do further analyses of the systems. Other data that must be managed includes data from contractors for out of house efforts.

All changes must be tracked and traceable from the origin to their verified implementation. Historical records are critical to project team members to be able to understand why changes were made and the intent of those changes after time has passed. In the event of an investigation after some mishap, the documented change history is invaluable to understanding things that may have contributed. The change history also allows for lessons learned in similar situations, especially if a change was instituted due to a safety concern or safety concerns were identified during review of proposed changes.

The verification process is important to the SSP in terms of ensuring that hazard control verifications were implemented correctly and successfully as well as making sure that the configuration analyzed is indeed the configuration finally produced. If not, the CM and DM processes have broken down and need to be evaluated. The breakdown could be a process breakdown or an implementation breakdown where discipline team members did not properly process or participate in change activity.

Summary

The System Safety Professional plays a vital role in the safe and successful implementation and execution of a program or project. Inherent in that role is participation in the formal configuration and data management processes. The SSP is involved in the identification of configuration controlled items and interfaces, the evaluation of safety impacts of designs and changes made thereto, the tracking and control of changes to the baseline and the verification that the project documentation and product reflect the design requirements and modifications made thereto. The SSP is also involved in identifying required data and having insight into the data processes to make sure accurate information and records are maintained from both contractor and in-house activities. The SSP must, in short, act as a fully involved discipline team member to ensure that the product built or delivered is the product analyzed using the actual design details that reflect the real status of the hardware or software.

1. "*Configuration Management*," NASA Site for On-Line Learning and Resources.

2. "*Data Management*," NASA Site for On-Line Learning and Resources.

3. NASA Program Control Skill Course - *Configuration Management*, 1/30/95.

Note: Reference 1 was relied on heavily for the production of this paper for descriptions of the configuration and data management processes. The System Safety roles are based on the author's experience.. This paper does not represent official positions of NASA or Marshall Space Flight Center.

Biography

Charles Herbert Shivers, PhD, P.E., CSP, ED43,
Marshall Space Flight Center, AL 35812.
Telephone (256)544-8903, Facsimile (256)544-7292, email:herb.shivers@msfc.nassa.gov
Dr. Shivers is Deputy Group Lead, Configuration and Data Management (C&DM) Group, Engineering Systems Department, of the

MSFC Engineering Directorate. Before his current assignment, Dr. Shivers had over 25 years experience in Industrial and Systems Safety for the Department of the Army, the Tennessee Valley Authority and NASA. The C&DM Group provides C&DM services for all of MSFC programs and projects through a centralized, co-located approach. Dr. Shivers earned degrees from Auburn University, Bachelor of Industrial Engineering;
Texas A&M University, Master of Engineering, Industrial Engineering; and University of Alabama in Huntsville, Doctor of Philosophy, Industrial and Systems Engineering and Engineering Management. He is a member of Alpha Pi Mu and Tau Beta Pi honor societies. Dr. Shivers is a member of the System Safety Society and the Tennessee Valley Chapter and is a registered Professional Engineer in Alabama and a Certified Safety Professional. He is also a member of the American Society of Safety Engineers and has contributed articles to the Professional Safety Magazine:

"Halos, Horns, and Hawthorne," Professional Safety, March 1998.

"Self-Directed Work Teams and Safety Performance," *Professional Safety*, July 1999.